Department of Homeland Security Daily Open Source Infrastructure Report for 22 March 2006

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports eight former employees of Southwest Airlines have been charged with wire fraud after allegedly stealing more than $1 million from the company in a scheme involving used tickets. (See item 13)

- Reuters reports U.S. researchers said on Monday, March 20, that the H5N1 strain of bird flu in humans has evolved into two separate strains, which could complicate developing a vaccine and preventing a pandemic. (See item 25)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base

Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping

Sustenance and Health: Agriculture; Food; Water; Public Health

Federal and State: Government; Emergency Services

IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard

Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *March 21, Calgary Herald (Canada)* — **Protected places opened to drilling.** The Alberta, Canada government has paved the way for coal bed methane drilling in the world's largest swath of aspen parkland, which the province set aside to protect a decade ago. Well proposals have yet to go before Alberta's energy regulator, but the province has approved several applications from oil and gas companies to access Rumsey Parkland, said Alberta Community Development spokesperson Cheryl Robb. Near Waterton, Suffield, and Rumsey, special designations don't guarantee complete protection. Rumsey, for example, was declared a Special Place in 1996 by the Alberta government. But the parkland lies in Alberta's largest coal bed

methane−producing zone, offering a form of natural gas that's harder to extract. The Nature Conservancy of Canada's Waterton Park Front is undergoing seismic testing for natural gas. The organization anticipates drilling proposals will follow shortly. The federal government is considering EnCana Corp.'s proposal to drill nearly 1,300 gas wells in Suffield National Wildlife Area near Medicine Hat. The area, which includes 92 species of plants and animals listed as at risk or threatened, was included in the Canada Wildlife Act three years ago.
Source: http://www.canada.com/calgaryherald/news/city/story.html?id=49fb97fa−91de−455c−a0a4−9b721e9a9066

2. *March 21, Canadian Press* — **Proposed Canadian pipeline spurs Arctic coal gasification mega−plan.** A proposed Mackenzie Valley natural gas pipeline in Canada is still before the regulators and it's already creating massive new plans for industrial development in the Arctic. Vancouver−based West Hawk Development has unveiled plans to strip−mine extensive coal reserves along the Mackenzie River and begin building $2 billion worth of coal gasification plants to tie into the pipeline within four years. Earlier this month, West Hawk announced it had bought leases in three areas of the Northwest Territories estimated to contain 2.1 billion tons of coal. West Hawk president Mark Hart said the coal could be barged to market along the Mackenzie River. But gasification −− turning the coal through heat and pressure into synthetic natural gas −− is West Hawk's priority. Hart envisions a series of strip mines taking up to 30 million tons of coal a year and feeding it into gasification plants. The plants would be developed in four phases, with each phase worth about $450 million. That gas would be shipped to southern markets in the pipeline proposed by Imperial Oil and its partners, which is now the subject of public hearings by two regulatory boards.
Source: http://www.canada.com/vancouversun/news/business/story.html?id=ec9c0700−09b9−4f92−9335−393058fb010a&k=31468

3. *March 21, Government Computer News* — **Energy labs test grid for monster downloads.** Two Department of Energy laboratories and a number of universities tested a grid network that will eventually distribute experimental data from the CERN particle physics laboratory in Geneva, Switzerland, to multiple research laboratories around the globe. This test showed how terabytes of data generated at CERN could be dispersed to multiple laboratories. It showed such bulk transfers are possible, using grid software. In 2007, CERN will crank up the Large Hadron Collider, which will be the world's largest particle accelerator. The physics community wants to channel the collision results to labs worldwide. This approach may tap the potential power of distributed computing. Grid tools are essential for the job, said Ian Fisk, associate scientist at the Department of Energy's Fermi National Accelerator Laboratory. For instance, Fermilab uses Storage Resource Manager (SRM). "The SRM interface allows us to describe that large group of servers as an interface," Fisk said. CERN sends the data from multiple servers, which are received by the numerous servers at Fermilab. SRM lends a hand in load balancing, traffic shaping, performance monitoring, authentication, and resource usage accountability as well.
Source: http://www.gcn.com/online/vol1_no1/40188−1.html

4. *March 21, Journal News (NY)* — **Feds to probe tritium leaks at nuke plants nationwide.** Federal regulators hope a new task force will determine whether the release of radioactive tritium at nuclear plants is part of a national trend and requires changes in oversight policy. The Nuclear Regulatory Commission (NRC) on Monday, March 20, announced the panel, made up of 11 agency experts and one from a yet−to−be−determined state, to examine the issue of

accidental, unmonitored releases of tritium from the nation's 103 plants. "Indian Point is a factor in deciding to do this," NRC spokesperson Neil Sheehan said. The NRC is still in the midst of a special investigation into the source of the Indian Point tritium leak, which plant and agency officials believe originates from a spent−fuel storage pool. The panel is expected to complete its report by August 31 and will look at the potential public−health impact from tritium releases; how the releases were communicated to the public, state and local officials, federal agencies, Congress, and others; other inadvertent releases at nuclear power plants, including decommissioning sites, from 1996 to the present; industry action in response to the releases, including the timing of remediation efforts; and NRC oversight of accidental releases.
Source: http://www.lohud.com/apps/pbcs.dll/article?AID=/20060321/NEWS02/603210351/1204

5. *March 20, Government Computer News* — **IG: Energy Department lost computer equipment.** At least 18 pieces of "computer processing equipment," including at least one laptop, are missing from the Department of Energy's (DOE) Office of Intelligence (IN), and department officials do not know whether any of it contained classified information, according to a new report from DOE's inspector general (IG). The IG's investigation found that: Officials could not locate 18 items of sensitive computer processing equipment and were unable to determine if the missing items contained classified information; officials had not reported missing sensitive property to the Office of Security; and more than 280 pieces of sensitive property had not been entered into the IN's inventory records. IN had no accreditation documentation for the laptop because it was "legacy" equipment. As for the other 17 missing items, "computers that are attached to an accredited network are not individually accredited and IN does not maintain historical records indicating which equipment processed classified information," IG Gregory Friedman wrote. When IN disposes of computer equipment, all pieces are treated as if they had handled classified information, but no records indicated disposal of the equipment.
Source: http://www.gcn.com/online/vol1_no1/40184−1.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

6. *March 21, Boston Channel* — **Officials investigate hospital chemical leak.** A chemical incident at Boston Medical Center prompted the evacuation of 200 people Monday night, March 20. The medical center's Mallory Building was evacuated as authorities examined the circumstances surrounding the leak, which forced dozens of the city's homeless from the nearby Woods Mullen Shelter onto the streets. The facility was later deemed safe enough for people to re−enter. Homeless evacuees were also permitted back inside the shelter.
Source: http://www.thebostonchannel.com/consumer/8157601/detail.html

7. *March 20, KSL News (UT)* — **Ammonia leak forces evacuation of Costco Warehouse.** Salt Lake City, UT, Hazmat crews responded to a gas leak in a refrigeration system Monday morning, March 20, at the Costco Warehouse. About 80 employees were evacuated from the building, while 300−South was closed at 60th West for several hours.
Source: http://www.ksl.com/?nid=148&sid=178719

[Return to top]

Defense Industrial Base Sector

8. *March 21, Defense Industry Daily* — **U.S. debating aerial tanker types.** It has been a long road for the U.S. aerial tanker replacement competition. After the Darlene Druyun scandal and the linked but separate withdrawal of Boeing's KC−767 lease proposal, the U.S. continues to examine its options. Some reports note that the existing tanker fleet of "more than 490" KC−135 Stratotankers derived from Boeing 707s, and 59 KC−10 Extenders derived from McDonell Douglas DC−10−30CFs, may be able to perform until 2040. Yet a combination of procurement momentum and steadily increasing, future−uncertain maintenance costs for the Air Force's aging Boeing 707 fleets continues to push the competition ahead. With a Request For Information approaching, industry−watchers are paying attention again. The question becomes twofold: what to replace the existing fleet with, and when to do so. The question of what to replace the existing fleet with is far less clear. A RAND report discarded a number of alternatives, and leaves the Air Force looking at manned derivatives of commercial aircraft, in the medium to large size range. In addition, the Pentagon has yet to finalize its tanker replacement requirements.
Source: http://www.defenseindustrydaily.com/2006/03/us−debating−aerial−tanker−types−mix/index.php#more

[Return to top]

Banking and Finance Sector

9. *March 20, Channel Register (UK)* — **Forgotten password clues create hacker risk.** Security flaws in the "forgotten password" feature of e−commerce Websites leave half the UK's online retailers open to attack, according to security consultant SecureTest. It warns that the log−in process of many transactional Websites can be subverted by a "brute force" or enumeration attack. In a survey of 107 popular online retail Websites in the UK, SecureTest found that 54 of the sites are potentially vulnerable to this type of hack attack. Differences in responses by applications when valid and invalid user account names can give clues to hackers and form the basis of enumeration attacks. If a valid user name (or registered e−mail address) is entered on a "forgotten password" page, a Web application might respond stating that a password will be sent to the user by e−mail. If an invalid user name is entered, the application could respond with "invalid account name". Using this information, a script can be written to try numerous account names, exploiting these differences in response. With a list of valid user names, a hacker might target the application and crack account passwords, then log into an account, make purchases or extract confidential data, such as credit card details.
Source: http://www.channelregister.co.uk/2006/03/20/forgotten_passwo rd_security_risk/

10. *March 19, Websense Security Labs* — **Crimeware, Trojan redirector targeting more than 100 banks.** Websense Security Labs has received reports of a Trojan Horse which targets users of more than 100 financial institutions in the United States and Europe. Once installed on a user's machine, the malicious code checks to see if there is an active window open (either "my

computer" or Internet Explorer). If one of these applications is not open, the malicious code modifies the contents of the hosts file on the local machine with a list of sites all pointing to localhost (127.0.0.1). If either of these applications is open, the behavior is different. In this case, the malicious code performs a DNS lookup to a DNS server hosted in Russia and receives an address for a Website. The address returned from that DNS server is then populated into the hosts file along with a list of target brands. If the target machine visits one of the sites in the list, the machine is redirected to a fraudulent Website on the hosted machine in Russia. This allows the attacker to change the destination address through DNS if one of the servers is taken offline.
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =447

11. *March 18, Websense Security Labs* — **Phishing Alert: Gold Coast Federal Credit Union.** Websense Security Labs has received reports of a new phishing attack that targets customers of Gold Coast Federal Credit Union. Users receive a spoofed e−mail message, which claims that their account information needs to be verified due to new security measures. The message provides a link to a phishing Website. Users who visit this Website are prompted to enter personal and account information.
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =446

12. *March 17, Internal Revenue Service* — **IRS: Updated phishing, identity theft, and scam warning.** The Internal Revenue Service has issued several consumer warnings on the fraudulent use of the IRS name or logo by scammers trying to gain access to consumers' financial data in order to steal their assets. The following are examples of recent schemes: e−mails claiming to come from tax−refunds@irs.gov, admin@irs.gov, or other variations on the irs.gov theme which tell the recipients that they are eligible to receive a tax refund for a given amount; the Treasury Inspector General for Tax Administration has reported that it found 12 separate Websites in 18 different countries hosting variations on this scheme; and a bogus IRS letter and Form W−8BEN (Certificate of Foreign Status of Beneficial Owner for United States Tax Withholding) which asks non−residents to provide personal information such as account numbers, PINs, mother's maiden name, and passport number. The legitimate IRS Form W−8BEN, which is used by financial institutions to establish appropriate tax withholding for foreign individuals, does not ask for any of this information.
Source: http://www.irs.gov/newsroom/article/0,,id=154848,00.html

[Return to top]

Transportation and Border Security Sector

13. *March 21, Associated Press* — **Former Southwest Airlines employees charged in ticket scam.** Eight former employees of Southwest Airlines have been charged with wire fraud after allegedly stealing more than $1 million from the company in a scheme involving used tickets. The workers would issue already−used tickets to customers who paid cash, giving the traveler a ticket that should have been voided in Southwest's systems, according to a federal grand jury indictment, returned last week. Investigators said the Southwest workers, employed at El Paso International Airport, collected cash on transactions from March 2000 through January 2003. Brandy King, a spokesperson for Dallas−based Southwest, said no passengers were stuck with worthless tickets from the scheme. She said the agents recorded cash ticket purchases as

exchanges and pocketed the money. Southwest has since changed its controls to prevent similar abuse.
Source: http://www.usatoday.com/travel/flights/2006−03−21−swa−ticket s_x.htm

14. *March 21, Shanghai Daily (China)* — **United Airlines expands codeshare to Shanghai.** United Airlines, the largest carrier on Sino−U.S. routes, signed a codeshare agreement with Shanghai Airlines yesterday as both carriers cooperate further to expand destination options and frequent flyer business. The two airlines agreed to codeshare nine flights starting on May 15, which is still pending U.S. government approval, they said on Monday, March 20, in Shanghai. As part of the deal, Shanghai Airlines, China's fifth biggest carrier, will codeshare with Chicago−based United on five flights from the city to San Francisco and Chicago, Chicago to New York, San Francisco to New York, and San Francisco to Los Angeles. United will codeshare with Shanghai Airlines on flights from Pudong International Airport to Chengdu in Sichuan Province, Qingdao in Shandong Province, Shenyang and Dalian in Liaoning Province.
Source: http://www.shanghaidaily.com/art/2006/03/22/252987/Airlines_ expand_codeshare.htm

15. *March 21, Department of Transportation* — **Train accidents and derailments decline in 2005.** Amid a strong economy and increased demand for rail services in 2005, the number of overall train accidents and derailments declined according to the latest statistics compiled by the Federal Railroad Administration, Department of Transportation Secretary Norman Y. Mineta announced on Tuesday, March 21. Preliminary full year data comparing 2005 with 2004 shows that overall train accidents decreased 7.9 percent, including an 8.4 percent reduction in the number of derailments, Mineta said. In addition, the total number of highway−rail grade crossing fatalities declined 3.5 percent and the grade crossing collision rate reached an all−time record low of 3.81 per million train−miles, Mineta said. The preliminary data also reveals that human−factor caused train accidents −− the leading cause of all train accidents −− decreased 12.8 percent last year, he said. The rail employee on duty injury rate also dropped 12.7 percent while train−to−train collisions increased 8.4 percent, Mineta added. In addition, trespassing remains the largest single cause of rail−related fatalities accounting for 53.7 percent of the total. To further improve railroad safety performance, Mineta launched a National Rail Safety Action Plan in May 2005 to target the most frequent and highest risk causes of train accidents.
Source: http://www.dot.gov/affairs/dot4006.htm

16. *March 21, Associated Press* — **Minuteman Project plans new border patrol.** A controversial civilian border patrol group is planning a return to Arizona in two weeks to again confront the problem of illegal immigration. Some say the original Minuteman Project conducted in April 2005 in Cochise County and a subsequent patrol in October brought increased national attention to the Arizona stretch of the U.S.−Mexico border. Minuteman president Chris Simcox said that his group will continue to plan month−long patrols every six months as long as needed. Simcox said he is expecting about 1,000 Minuteman Civil Defense Corps volunteers in Arizona for the next patrol, expected to start April 1 and last for one month. He said the group chose to patrol the Altar Valley this time because it is the most heavily trafficked corridor this fiscal year. The group will also conduct patrols in New Mexico, Texas, and California on the U.S.−Mexico border, and in Washington state, New York, and Vermont on the U.S.−Canada border, Simcox added.
Source: http://www.cbsnews.com/stories/2006/03/21/ap/national/mainD8 GG0S384.shtml

17. *March 17, GovExec* — **Customs bureau may seek private sector help.** U.S. Customs and Border Protection only has 80 inspectors to validate the security plans for about 10,000 companies that have applied to be part of the Customs−Trade Partnership Against Terrorism (C−TPAT) program, Jayson Ahern, the agency's assistant commissioner of field operations, told the House Homeland Security Economic Security Subcommittee at a hearing on Thursday, March 16. For the first time, the agency is considering hiring private companies to validate the security plans of some companies that primarily work out of countries with a low risk of terrorism activity, Ahern said. Under the C−TPAT program, which was established after the September 11, 2001, terrorist attacks, companies voluntarily give the U.S. government detailed information about the security of their supply chain in order to have convenient access to U.S. ports. Ahern said C−TPAT is one of five main programs aimed at increasing security, adding that the nation's 322 ports are "far safer today than before 9/11."
Source: http://www.govexec.com/story_page.cfm?articleid=33628&dcn=to daysnews

[Return to top]

Postal and Shipping Sector

18. *March 21, Messenger−Inquirer (KY)* — **Midline Air Freight expanding in Kentucky.** Springfield, KY−based Midline Air Freight hopes to move into a hangar at Owensboro−Daviess County Regional Airport by June, creating eight to 10 jobs. The airport board Monday, March 20, approved a lease on the hangar in the name of Midline's parent company, Georgia−based CorpJet. Midline hauls freight for UPS as well as newspapers for the New York Times and the Wall Street Journal. That's the main reason for the $12 million airport expansion −− which includes a 1,500−foot extension of the north−south runway to 8,000 feet −− that's scheduled for completion in 2007. The airport has been courting cargo operations since 1988−89.
Source: http://industrywatch.yellowbrix.com/pages/iw/customer/Story.nsp?story_id=90876554&ID=iw&scategory=Transportation&H=Cargo+Company+Coming+This+Summer&

[Return to top]

Agriculture Sector

19. *March 21, New York Times* — **Poultry industry prepares for the possibility of avian flu in the U.S.** The H5N1 strain of avian flu has not been found anywhere in the Western Hemisphere, but Mark Holden, a chicken grower for Tyson Foods in Ellijay, GA, is not taking any chances. Every seven weeks a group of his chickens is tested before the birds are sent to be slaughtered. All people who enter or leave the chicken houses must walk through disinfecting baths. And visitors and workers must wear plastic booties over their shoes. Poultry producers doubt that their chickens will be infected by avian flu or that people would catch the virus even if there were contamination. But they are concerned that if the virus gets to the U.S., people will eat less chicken, simply out of fear. And they are revving up big plans to be prepared. The stakes are enormous. U.S. poultry producers like Tyson, Pilgrim's Pride, and Gold Kist sell 26

billion pounds of chicken each year. Tyson and Pilgrim's Pride say they have formed internal avian flu task forces that meet regularly and include top executives and leaders from different departments. These executives have been meeting with government health officials, discussing what information should go on the companies' Websites and when, and devising sales loss projections.
Source: http://www.nytimes.com/2006/03/21/business/21poultry.html?hp&ex=1143003600&en=c238275775518650&ei=5094&partner=homepage

20. *March 20, U.S. Food and Drug Administration* — **Food and Drug Administration prohibits use of antiviral drugs in poultry.** The U.S. Food and Drug Administration (FDA) Monday, March 20, published a proposed final rule to prohibit the extralabel use in poultry of two classes of approved human antiviral drugs in treating influenza. FDA is taking this measure to help preserve the effectiveness of these drugs for treating or preventing influenza infections in humans. Specifically, the order prohibits the extralabel use by veterinarians of anti−influenza adamantane (amantadine and rimantadine) and neuraminidase inhibitor (oseltamivir and zanamivir) drugs in chickens, turkeys, and ducks. Extralabel use is the actual use or intended use of a drug in an animal in a manner that is not in accordance with the approved labeling. FDA may add other animal species to the prohibited list as new data becomes available.
Source: http://www.fda.gov/bbs/topics/NEWS/2006/NEW01339.html

21. *March 20, Xinhua (China)* — **Brazil ends foot−and−mouth disease slaughter in southern state.** Brazil's Agriculture Ministry announced on Monday, March 20, that it had completed the cull of animals infected with foot−and−mouth disease in the southern state of Mato Grosso do Sul, around five months after the disease was discovered. The disease, detected in October 2005, triggered embargoes by 50 countries on Brazilian beef.
Source: http://news.xinhuanet.com/english/2006−03/21/content_4325772 .htm

[Return to top]

Food Sector

22. *March 22, Associated Press* — **Food poisoning caused by strain used in biological weapons investigated.** An expert from the U.S. Center for Disease Control and Prevention is investigating an outbreak of food poisoning in Thailand after a finding that the bacteria that caused it is the same strain used to produce biological weapons, officials said Tuesday, March 21. Last week, 143 people suffered stomach pains, vomiting, and muscle weakness after eating fermented bamboo shoots at a temple fair in the northern Thai province of Nan, and 39 remain in critical condition, said Prajaya Boonyawongwiroje of the Public Health Ministry. Thai officials say U.S. experts are eager to study such outbreaks of botulism to strengthen preparedness for biological weapons attacks.
Botulism information: http://www.bt.cdc.gov/agent/botulism/
Source: http://english.ohmynews.com/ArticleView/article_view.asp?no= 280655&rel_no=1

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

23. *March 21, Reuters* — **Pakistan confirms bird flu.** Pakistan on Tuesday, March 21, became the latest country to confirm bird flu in poultry. Pakistan said the bird flu virus found in two poultry flocks late last month was the H5N1 strain. But livestock Commissioner Muhammad Afzal said there had been no other cases of bird flu since the outbreak was first reported on February 27 at farms in the North West Frontier Province and there were no cases of humans being infected.
Source: http://abcnews.go.com/International/wireStory?id=1749895

24. *March 21, Agence France−Presse* — **Five die of bird flu in Azerbaijan.** The dangerous strain of H5N1 bird flu has killed five people in Azerbaijan since late February, the World Health Organization (WHO) said, warning that the cause of some of the cases was still unknown. A total of seven patients had tested positive for infection with the highly pathogenic strain of avian influenza in the southeast and west of the country, the WHO said Tuesday, March 21. Tests were underway on two other patients with pneumonia−like symptoms from the same area as six of the confirmed cases.
Source: http://news.yahoo.com/s/afp/20060321/hl_afp/healthfluazerbai jan_060321161246

25. *March 20, Reuters* — **U.S. study defines two clear bird flu strains.** The H5N1 strain of bird flu in humans has evolved into two separate strains, U.S. researchers reported on Monday, March 20, which could complicate developing a vaccine and preventing a pandemic. One strain, or clade, made people sick in Vietnam, Cambodia, and Thailand in 2003 and 2004 and a second, a cousin of the first, caused the disease in people in Indonesia in 2004. Two clades may share the same ancestor but are distinct, the team from the U.S. Centers for Disease Control and Prevention found. Speaking to the International Conference on Emerging Infectious Diseases in Atlanta, Rebecca Garten, who helped conduct the study, said the pool of H5N1 candidates with the potential to cause a human influenza pandemic is getting more genetically diverse, which makes studying the virus more complex and heightens the need for increased surveillance.
Source: http://www.alertnet.org/thenews/newsdesk/N2012779.htm

26. *March 20, U.S. Department of Agriculture* — **Screening for highly pathogenic H5N1 avian influenza in migratory birds expanded.** Secretary of Agriculture Mike Johanns, Secretary of the Interior Gale A. Norton and Secretary of Health and Human Services Michael Leavitt on Monday, March 20, moved to further ensure the protection of people, domestic poultry, and wild birds by unveiling an enhanced national framework for early detection of highly pathogenic avian influenza (HPAI) in wild migratory birds in the U.S. The interagency plan outlines five specific strategies for early detection of the virus in wild migratory birds, including: investigation of disease−outbreak events in wild birds, expanded monitoring of live wild birds, monitoring of hunter−killed birds, use of sentinel animals, such as backyard poultry flocks, and environmental sampling of water and bird feces. In 2006, USDA and its cooperators plan to collect between 75,000 to 100,000 samples from live and dead wild birds. They also plan to collect 50,000 samples of water or feces from high−risk waterfowl habitats across the U.S.

Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2006/03/0095.xml

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

27. *March 21, Charleston Gazette (WV)* — **Evacuees could flood West Virginia in an emergency.** Should the nation’s capital come under attack, how would West Virginia manage what disaster planners call a “western migration” of evacuees streaming into the state? That was one of a number of topics addressed Monday, March 20, during the West Virginia Summit on Homeland Security. Since the Atlantic Ocean blocks an eastern escape route from the nation’s capital, and urban areas to the north and south might be viewed as potential targets, a “western migration” of evacuees seems to be a likely response to a nuclear or biological attack. West Virginia would be the likely first stop in such a migration. With the nation’s fourth−largest metropolitan area, with nearly seven million people, so close at hand, “if just a small percentage comes to West Virginia, we see our services being overwhelmed,” said James Spears, West Virginia’s military affairs and public safety secretary. As a precaution, Spears said federal officials have identified several places in West Virginia as potential temporary government sites, in the event of an attack on Washington.
Source: http://wvgazette.com/section/News/2006032020

28. *March 20, Congress Daily* — **Chertoff vows feds won't supersede local responders.** Department of Homeland Security Secretary Michael Chertoff said Monday, March 20, that the federal government has a responsibility to ensure that front−line responders have the necessary vaccines to defend against biological threats, but added that he has no intention of superseding state and local emergency responders in handling a wide range of future disasters. "The idea is to carefully understand your requirements, assess your capabilities, work with you to figure out what additional capabilities you need, and then draw upon the capabilities we have at the federal government to support you," he said. In addition, he challenged state and local responders to extend their training and exercises to cover non−traditional threats.
Source: http://govexec.com/story_page.cfm?articleid=33640&dcn=todays news

29. *March 20, WLOX 13 (MS)* — **Hurricane experts meet in Alabama to discuss 2006 hurricane season.** Governmental agencies, hurricane experts, and emergency officials from all over the nation are meeting in Mobile, AL, this week for the 60th Interdepartmental Hurricane Conference. Federal Coordinator for Meteorology Sam Williamson says the first improvement needs to be in communication and making sure the public is fully aware of the dangers lurking at sea. Dr. Jack Beven, from the National Weather Center, says there is a need to improve storm intensity forecasting models. "Sometimes we get false alarms of rapid intensification from our computer models, other times the models don't show that much development and we get it

anyway," Beven says.
Source: http://www.wlox.com/Global/story.asp?S=4657591&nav=6DJI

[Return to top]

Information Technology and Telecommunications Sector

30. *March 20, Hackers Center* — **Internet Explorer multiple event handlers denial−of−service weakness.** There is a weakness in Internet Explorer, which can be exploited by malicious people to cause a denial−of−service. Analysis: The vulnerability is caused due to an array boundary error in the handling of HTML tags with multiple event handlers. This can be exploited to crash a vulnerable browser via a HTML tag with 94 or more event handlers. Affected software: Microsoft Internet Explorer 6.x. Solution: Do not visit untrusted Websites.
Source: http://www.hackerscenter.com/archive/view.asp?id=23679

31. *March 20, Securi Team* — **Paper on Domain Name System amplification attacks released.** In recent months several attackers massively exploited recursive name servers to amplify distributed denial−of−service (DDoS) attacks against several networks utilizing IP spoofing. Analysis of three of these attacks makes up the bulk of a recent study released Friday, March 17. The paper outlines a DDoS attack which abuses open recursive Domain Name System name servers using spoofed UDP packets.
To access the full report: http://www.isotf.org/news/DNS−Amplification−Attacks.pdf
Source: http://www.securiteam.com/securityreviews/5GP0L00I0W.html

32. *March 20, IDG News Service* — **Panel explores roots of spyware, adware.** Following the money trail behind the flood of spyware and adware on the Internet poses some sticky questions around liability, said a panel of spyware experts at a workshop in New York City Friday, March 17. Legal experts, government officials and technology professionals gathered at New York University School of Law to discuss the causes of and solutions to unwanted software programs that track Internet users' behavior. One panelist suggested that companies advertising online should develop more thorough policies to control where their ads go on the Internet.
Source: http://www.infoworld.com/article/06/03/20/76629_HNspywarepan el_1.html

33. *March 20, GovExec* — **OMB expands technology consolidation effort.** The Office of Management and Budget (OMB) is pressing forward with its effort to consolidate and centralize federal information technology systems, despite admitting that not all the details are resolved. OMB last week kicked off three governmentwide task forces to review additional areas −− called "lines of business" −− it has deemed potentially ripe for consolidation. The areas that will be examined are: IT infrastructure, geospatial systems, and systems for budget formulation and execution.
Source: http://govexec.com/story_page.cfm?articleid=33638&dcn=todays news

34. *March 16, Associated Press* — **ICANN to test Chinese, Arabic domain names.** The Internet's key oversight agency, Internet Corporation for Assigned Names and Numbers, has outlined a plan for testing domain names entirely in non−English characters. The tests would help ensure that introducing non−English suffixes wouldn't wreck a global addressing system that millions

of Internet users rely upon every day. The Internet's main traffic directories know only 37 characters.
Source: http://www.foxnews.com/story/0,2933,188121,00.html

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of several vulnerabilities in Adobe Macromedia Flash products. A system may be compromised if a user accesses a web page that references a specially crafted Flash (SWF) file. Successful exploitation may allow a remote attacker to execute arbitrary code with the privileges of the user. For more information please review the following:

VU#945060 − Adobe Flash products contain multiple vulnerabilities
http://www.kb.cert.org/vuls/id/945060

TA06−075A − Adobe Macromedia Flash Products Contain Vulnerabilities
http://www.us−cert.gov/cas/techalerts/TA06−075A.html

Adobe Security Bulletin: APSB06−03
http://www.macromedia.com/devnet/security/security_zone/apsb 06−03.html

Microsoft Security Advisory: 916208
http://www.microsoft.com/technet/security/advisory/916208.ms px

US−CERT encourages administrators to apply the appropriate updates, patches, or fixes as soon as possible.

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 113 (auth), 32459 (−−−), 80 (www), 139 (netbios−ssn), 445 (microsoft−ds), 26777 (−−−), 1027 (icq), 135 (epmap) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

35.

March 21, Telematics Journal — **Pilot program features GPS on school buses.** Cutting−edge technology is making it easier for transportation directors to keep track of school buses. With the help of a global−positioning satellite (GPS) system installed in each of the school buses, school officials can locate where their buses are at all times. IC Corporation, the nation's largest school bus manufacturer, is pilot testing 10 school buses in New York that are outfitted with a factory−installed GPS solution that can monitor school bus locations in real−time and report back to school officials electronically on exact position and how well the bus is performing. "Security is its greatest benefit," said Chuck Tanzer, fleet manager for the Saratoga Springs City School District.
Source: http://www.telematicsjournal.com/content/newsfeed/6690.html

[Return to top]

General Sector

Nothing to report.

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.